

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-298449

(P2001-298449A)

(43)公開日 平成13年10月26日 (2001.10.26)

(51)Int.Cl.⁷

H 04 L 9/14

G 06 F 15/00

識別記号

330

F I

G 06 F 15/00

H 04 L 9/00

テ-マコード^{*}(参考)

3 3 0 A 5 B 0 8 6

6 4 1 5 J 1 0 4

審査請求 未請求 請求項の数40 O.L. (全 21 頁)

(21)出願番号

特願2000-110651(P2000-110651)

(22)出願日

平成12年4月12日 (2000.4.12)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 山口 雅史

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 田中 豊

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 100083172

弁理士 福井 豊明

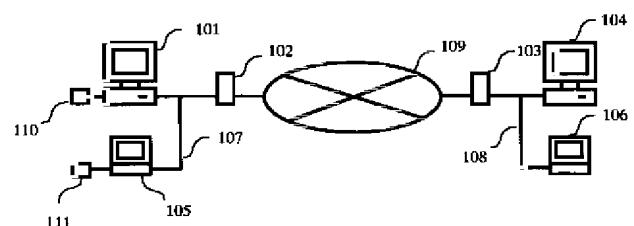
最終頁に続く

(54)【発明の名称】 セキュリティ通信方法、通信システム及びその装置

(57)【要約】

【課題】 データ送信を行うユーザごとにセキュリティ通信のレベルを設定でき、容易に各種セキュリティ通信の接続パラメータを変更でき、接続先とのセキュリティ通信のレベルを自動で設定するセキュリティ通信装置、システム、及び方法を提供する。

【解決手段】 通信端末を使用するユーザの情報とセキュリティ種を対応付けた対応情報を記憶し、上記対応情報からセキュリティ種を決定する。又、インターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶し、上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定する。さらに、セキュリティ種を所定のセキュリティ情報装置に問い合わせ、該問い合わせの回答に基づいて上記セキュリティ種を決定する。



【特許請求の範囲】

【請求項1】 送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信装置において、上記送信元通信端末を使用するユーザの情報とセキュリティ種を対応付けた対応情報を記憶する記憶手段と、上記ユーザの情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信装置。

【請求項2】 上記セキュリティ種選択手段が、さらに上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認する請求項1に記載のセキュリティ通信装置。

【請求項3】 上記セキュリティ種選択手段が決定するセキュリティ種が、セキュリティプロトコルの種類である請求項1又は2に記載のセキュリティ通信装置。

【請求項4】 上記セキュリティプロトコルが、IPS E Cである請求項3に記載のセキュリティ通信装置。

【請求項5】 上記セキュリティ種選択手段が決定するセキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項1又は2に記載のセキュリティ通信装置。

【請求項6】 上記定義情報群が、セキュリティポリシーである請求項5に記載のセキュリティ通信装置。

【請求項7】 上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも1つを含む請求項5に記載のセキュリティ通信装置。

【請求項8】 送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信システムにおいて、上記送信元通信端末を使用するユーザの認証を行うユーザ認証手段と、

上記ユーザとセキュリティ種を対応付けた対応情報を記憶する記憶手段と、

上記ユーザ認証手段により認証されたユーザの情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信システム。

【請求項9】 上記セキュリティ種選択手段が、さらに上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認する請求項8に記載のセキュリティ通信システム。

【請求項10】 ネットワークを介して接続される通信端末間の、通信のセキュリティを確保するセキュリティ通信方法において、

上記通信端末を使用するユーザの情報に基づいてセキュリティ種を決定することを特徴とするセキュリティ通信方法。

【請求項11】 送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキ

ュリティを確保するセキュリティ通信装置において、上記送信元通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶する記憶手段と、上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信装置。

【請求項12】 上記対応情報が、さらに上記送信元通信端末を使用するユーザの情報とセキュリティ種とが対応付けられているとともに、

上記ユーザの情報にも基づいて上記セキュリティ種を決定する請求項11に記載のセキュリティ通信装置。

【請求項13】 上記セキュリティ種の決定を、視覚化された上記セキュリティ種の一覧に対して同様に視覚化された上記インターネットアドレス情報を視覚的に対応付けることにより行う請求項11又は12に記載のセキュリティ通信装置。

【請求項14】 上記インターネットアドレス情報のIPアドレスへの変換に、ドメインネームシステムサーバを利用する請求項11に記載のセキュリティ通信装置。

【請求項15】 上記セキュリティ種が、セキュリティプロトコルである請求項11～14のいずれか1項に記載のセキュリティ通信装置。

【請求項16】 上記セキュリティプロトコルが、IP SECである請求項15に記載のセキュリティ通信装置。

【請求項17】 上記セキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項11～14のいずれか1項に記載のセキュリティ通信装置。

【請求項18】 上記定義情報群が、セキュリティポリシーである請求項17に記載のセキュリティ通信装置。

【請求項19】 上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも1つを含む請求項17に記載のセキュリティ通信装置。

【請求項20】 送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信システムにおいて、

上記送信元通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶する記憶手段と、

上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信システム。

【請求項21】 さらに上記送信元通信端末を使用するユーザの認証を行うユーザ認証手段を備えるとともに、上記対応情報が、上記送信元通信端末を使用するユーザの情報とセキュリティ種とが対応付けられ、上記ユーザの情報にも基づいて上記セキュリティ種を決

定する請求項20に記載のセキュリティ通信システム。

【請求項22】 上記セキュリティ種の決定を、視覚化された上記セキュリティ種の一覧に対して同様に視覚化された上記インターネットアドレス情報を視覚的に対応付けることにより行う請求項20又は21に記載のセキュリティ通信システム。

【請求項23】 ネットワークを介して接続される通信端末間の、通信のセキュリティを確保するセキュリティ通信方法において、

上記通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付け、

上記インターネットアドレス情報に基づいてセキュリティ種を決定することを特徴とするセキュリティ通信方法。

【請求項24】 通信端末を特定する端末特定情報と、該通信端末との通信において推奨されるセキュリティ種とを対応付けた対応情報を記憶する記憶手段と、
上記通信端末とは異なる端末からの、上記通信端末について推奨されるセキュリティ種の問い合わせに対し、上記端末特定情報に基づいて、上記対応情報から上記推奨されるセキュリティ種を選択する推奨セキュリティ種管理手段と、

上記選択された推奨されるセキュリティ種を送信する送信手段を備えることを特徴とするセキュリティ情報装置。

【請求項25】 さらに、上記端末特定情報が上記対応情報に無い場合に、上記通信端末に対して、該通信端末との通信において推奨されるセキュリティ種を問い合わせ手段を備える請求項24に記載のセキュリティ情報装置。

【請求項26】 上記セキュリティ種が、セキュリティプロトコルである請求項24又は25に記載のセキュリティ情報装置。

【請求項27】 上記セキュリティプロトコルが、IP SECである請求項26に記載のセキュリティ情報装置。

【請求項28】 上記セキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項24又は25に記載のセキュリティ情報装置。

【請求項29】 上記定義情報群が、セキュリティポリシーである請求項28に記載のセキュリティ情報装置。

【請求項30】 上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも1つを含む請求項28に記載のセキュリティ情報装置。

【請求項31】 送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保するセキュリティ通信装置において、
上記セキュリティの確保に用いるセキュリティ種を所定のセキュリティ情報装置に問い合わせる問い合わせ手段

と、

上記問い合わせに対応する上記所定のセキュリティ情報装置からの回答に基づいて上記セキュリティ種を決定するセキュリティ種選択手段を備えることを特徴とするセキュリティ通信装置。

【請求項32】 上記回答が、1又は複数の上記セキュリティ種を含む請求項31に記載のセキュリティ通信装置。

【請求項33】 上記セキュリティ種が、セキュリティプロトコルである請求項31又は32に記載のセキュリティ通信装置。

【請求項34】 上記セキュリティプロトコルが、IP SECである請求項33に記載のセキュリティ通信装置。

【請求項35】 上記セキュリティ種が、セキュリティ通信時に使用する定義情報群である請求項31又は32に記載のセキュリティ通信装置。

【請求項36】 上記定義情報群が、セキュリティポリシーである請求項35に記載のセキュリティ通信装置。

【請求項37】 上記定義情報群が、認証アルゴリズム又は暗号化アルゴリズムの少なくとも1つを含む請求項35に記載のセキュリティ通信装置。

【請求項38】 送信元通信端末からネットワークを介して接続される送信先通信端末へ送信される通信のセキュリティを確保する通信装置を備えるセキュリティ通信システムにおいて、
上記通信装置が、上記セキュリティの確保に用いるセキュリティ種を所定のセキュリティ情報装置に問い合わせる問い合わせ手段と、

上記問い合わせに対応する上記所定のセキュリティ情報装置からの回答に基づいて上記セキュリティ種を決定するセキュリティ種選択手段を備えるとともに、
上記所定のセキュリティ情報装置が、通信端末を特定する端末特定情報と、該通信端末との通信において推奨されるセキュリティ種とを対応付けた対応情報を記憶する記憶手段と、

上記通信端末とは異なる端末からの、上記通信端末について推奨されるセキュリティ種の問い合わせに対し、上記端末特定情報に基づいて、上記対応情報から上記推奨されるセキュリティ種を選択する推奨セキュリティ種管理手段と、
上記選択された推奨されるセキュリティ種を送信する送信手段を備えることを特徴とするセキュリティ通信システム。

【請求項39】 さらに、上記所定のセキュリティ情報装置が、上記端末特定情報が上記対応情報に無い場合に、上記送信先通信端末に対して該送信先通信端末との通信において推奨されるセキュリティ種を問い合わせる問い合わせ手段を備える請求項38に記載のセキュリティ通信システム。

【請求項40】 ネットワークを介して接続される通信端末間の、通信のセキュリティを確保する通信装置を備えるセキュリティ通信方法において、

上記通信装置が、該通信装置とは異なる通信装置について推奨されるセキュリティ種を所定のセキュリティ情報装置に問い合わせ、

上記所定のセキュリティ情報装置が、上記通信装置からの上記問い合わせに対し、上記推奨されるセキュリティ種を選択して上記通信装置に送信し、

上記通信装置が上記セキュリティ情報装置から送信された上記推奨されるセキュリティ種に基づいて上記セキュリティ種を決定することを特徴とするセキュリティ通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、セキュリティ通信方法に係り、詳しくは、必要に応じてセキュリティ種を変更可能なセキュリティ通信方法、通信システム及びその装置に関するものである。

【0002】

【従来の技術】近年、パーソナルコンピュータとインターネット技術の急激な普及により、容易でしかも安価にインターネット上に公開されるホームページによる情報提供及び情報収集が可能になっている。さらにこれだけにとどまらず、インターネットあるいは企業間のインターネットを介した電子メールの交換や、これらを利用した電子商取引や電子決済が一般化しつつある。このようなサービスを利用する場合、特に重要な情報を含む通信には専用線並のセキュリティの確保が重要である。

【0003】上述したようなセキュリティを確保する技術として、例えばインターネットのような広域ネットワークを仮想私設網とするVPN(Virtual Private Network)技術等のセキュリティ通信技術が注目されている。VPNを実現するセキュリティ通信のための接続手順としてトンネリングプロトコルがあり、L2F(Layer 2Forwarding)、PPTP(Point-to-Point Tunneling Protocol)、L2TP(Layer 2 Tunneling Protocol)、ATMP(Ascend Tunnel Management Protocol)、BayDV(S) (BayStream Dial VPN Service)、IPSEC(Internet Protocol Security Protocol)等が提案されている。上記セキュリティ通信のためのプロトコルを使用することにより、第3者が通信等を盗聴しうる上記広域ネットワークにおいて通信等のセキュリティを確保する事が可能となる。

【0004】これらの技術のうち、上記IPSECは、ネットワーク層(OSI参照モデル(Open System Interconnection reference model)第3層)で認証、暗号化を行うセキュリティプロトコルで、インターネット技術標準化委員会(IETF)で標準化されている(RFC2401から2412、2451)。上記IPSEC機

能を搭載したコンピュータや、ネットワーク接続装置であるルータ等を介してインターネットに接続することにより、上記VPNを構築することが可能である。即ち、ユーザはネットワークの種類を意識することなく、安全にインターネットを利用することができる。尚、IPSECを利用した通信を行うにあたっては、どのような認証アルゴリズムや暗号化アルゴリズムを使用するか、あるいはどのような暗号化鍵を使用するなどを、事前に送信側と受信側のIPSEC機能を搭載したコンピュータまたは、ネットワーク接続装置が整合を取っておく必要がある。この認証、暗号化アルゴリズムの整合をとるための相互通信を、セキュリティ通信のための接続と呼ぶ。IPSECにおいては、この接続はSA(Security Association)によって実現されている。上記SAは認証とセキュアメッセージ交換の機能を提供する基本的な枠組であり、通信のコンテキストを確立し、その通信のセキュリティのいくつかの側面を定義する。

【0005】以下に、図14、図15、図17、図18を参照しながら、従来の、セキュリティ通信としてIPSECを用いた通信方法について説明する。又、ここに通信端末とは、ネットワーク接続装置及びコンピュータを含む。

【0006】図14は、従来のセキュリティ通信としてIPSEC機能を搭載したルータを使用してVPNネットワークを構成したネットワークシステムの概略図、図15は、上記IPSEC機能を搭載したネットワーク接続装置間でのセキュリティ通信の接続手順を表した図、図17は、従来技術におけるIPSECの処理方針を決めるデータベースであるSPD(Security Policy Database)の例、図18は、従来技術におけるSAデータベースであるSAD(Security Association Database)の例である。ここに、SPDとはセキュリティポリシーを構成するデータベースである。又、セキュリティポリシーとは、セキュリティを確保されたシステムへのアクセス規制のことであり、一般にセキュリティ要件、セキュリティ上のリスク、及びセキュリティの測定手段が含まれる。通信端末間のセキュリティを確保するシステムにおいては、セキュリティを適用する相手先通信端末を区別する情報、セキュリティを適用するかどうかの情報等を備える。尚、IPSECにおいては、セキュリティポリシーは上記SPDに記述され、該SPDには送信先通信端末のIPアドレス、IPSEC処理の有無、認証、暗号化アルゴリズム等の内容を記述した上記SAが格納されるメモリ上のアドレスの位置情報を備える。

【0007】コンピュータ1401はLAN1407(Local AreaNetwork)で他のコンピュータ1405及びネットワーク接続装置1402と接続されており、ネットワーク接続装置1402を経由して、外部のインターネット1409やインターネット等のWANに接続されている。このインターネット1409には他のネットワー

ク接続装置1403を介してコンピュータ1404、1406が接続されるLAN1408が接続されている。ここで、上記ネットワーク接続装置1402、1403は、ルータ、ゲートウェイ、プロキシサーバ等のファイアウォールやVPN専用装置等である。ここで、コンピュータ1401他は、パーソナルコンピュータ、ワークステーション、サーバ、ノート型パソコン、IP電話、IPテレビ電話、IP携帯電話等の通信機能をもつ端末であればよい。

【0008】ここでは上記ネットワーク接続装置1402、1403にIPSEC機能を搭載し、ネットワーク接続装置1402、1403間でIPSECによる通信を行うものとして説明する。また、上記コンピュータ1401及び1404にIPSEC機能を搭載し、上記コンピュータ1401、1404間でIPSECによる通信を行うことも可能である。さらに、同様にIPSEC機能を搭載した、コンピュータ1401とIPSEC機能を搭載しているネットワーク接続装置1403間でIPSECによる通信を行うことも可能である。

【0009】ところで、コンピュータ1401がインターネット1409を介してコンピュータ1404にデータを送信する場合には、予め上記ネットワーク接続装置1402、1403間において上記セキュリティ通信のための接続を行う必要がある。以下に該セキュリティ通信のための接続について説明する。

【0010】IPSEC通信を始めるにあたり、まず、IPSECの暗号鍵交換のためのプロトコルであるIKE (Internet Key Exchange)が用いられる。該IKEを使用した通信は、IKEフェーズ1とIKEフェーズ2とに分けて説明することができ、上記ネットワーク接続装置1402、1403間で行われる。尚、IKEによる自動鍵交換を行わず、手動で秘密鍵の交換を行ってよい。

【0011】上記IKEフェーズ1(1501)では、IKE自身が安全に通信を行うために、互いに利用可能なSA (Security Association)を確立するための情報を交換する。ここでSAとは、例えば、認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含む一連の定義情報群である。

【0012】次に、IKEフェーズ2(1502)では、前記IKEフェーズ1にて確立した上記SAを用いて、IPSEC通信用のSAに関する情報を交換する。ここで、IPSEC通信用のSAの一例について図18に示す。図18は、複数の上記SAである、SA-1(1802)～SA-M(1803)を含むSAD1801であり、さらに各SAにはアドレス情報1804、インデックス情報であるSPI1805(Security Parameters Index)、及びセキュリティパラメータであるSAP1806が含まれる。上記アドレス情報1804には送信先IPアドレス、送信先ポート番号、送信元I

Pアドレス、送信元ポート番号、プロトコル番号等が含まれる。又、上記SPI1805には、擬似乱数等が用いられ、上記SAP1806は、認証アルゴリズム、暗号化アルゴリズム、暗号化鍵等のセキュリティ通信のレベルに直接関連する情報を持つ。例えば上記SAP-1(1806)の場合、認証アルゴリズムとしてHMAC-MD5を、暗号化アルゴリズムとしてDES-CBSが含まれる。

【0013】上記IKEフェーズ2(1502)で行われるIPSEC通信用のSAに関する情報の交換は、具体的には、ネットワーク接続装置1402がネットワーク接続装置1403に対し、IPSEC通信に使用する上記SAの構成の提案を送信し、該ネットワーク接続装置1403は上記提案の中から受け入れ可能なSAを返信するものである。ここで、上記SAの構成の提案は、上記ネットワーク接続装置1402の後述するデータ記憶部2103に予め記憶されている認証アルゴリズム、暗号化アルゴリズム等を用いて構成される。上記ネットワーク接続装置1402がどの様な認証アルゴリズム、暗号化アルゴリズムを搭載しているかは、ネットワーク接続装置により異なる。また、予め上記ネットワーク接続装置1402が提案するSAを決めておくことも可能である。

【0014】上記SAの返信処理により、IPSEC通信に使用されるSAが確立される。上記確立されたIPSEC通信に使用されるSAの情報は、図18に示すSAD1801及び、図17に示すSPD1701に格納される。該SPD1701の構成は以下の例に示される。即ち、送信先IPアドレス1702、IPSEC処理の有無1703、上記SAD1801における各SAの位置を示すアドレスポインタ1704、及び上記送信先IPアドレス1702にデータを送信する場合に、IPSECパケットを送信すべき先の通信端末のIPアドレス1705である。ここで、上記IPアドレス1705は、具体的にはネットワーク接続装置1403のIPアドレスとなる。ここで、送信の通信端末がIPSEC機能を搭載している場合、上記IPアドレス1702が上記IPアドレス1705と同一となる。また、上記送信先IPアドレス1702及び1705は範囲指定が可能である。範囲指定とは、具体的にはIPアドレスを用いて例えば”192.168.1.1～192.168.1.100”という指定を指し、上記範囲指定により1つの指定で例えば200台の通信端末へのデータの送信を指定することが出来る。尚、上記SAは片方向で1つ設定されるので、双方通信の場合は独立したSAがネットワーク接続装置1402、1403にそれぞれ設定される。

【0015】上記IPSEC通信に使用されるSAが確立された後、送信側のコンピュータ1401から上記コンピュータ1404に送信されるデータは、該コンピュ

ータ1401にてIPヘッダを付加され、IPパケットとしてLAN1407を介してネットワーク接続装置1402に送られる。該ネットワーク接続装置1402は、後述するIPSEC処理を行うことにより上記IPパケットをIPSECパケット1503として、上記ネットワーク接続装置1403に送信する。上記IPSECパケット1503を受信した上記ネットワーク接続装置1403は、同じく後述するIPSEC処理にて上記IPSECパケット1503をIPパケットに戻し、上記LAN1408を介して上記コンピュータ1404に送信する。即ち、上記インターネット1409を介して接続される上記ネットワーク接続装置1402、1403間では、送信側のコンピュータ1401から上記コンピュータ1404に送信されるデータはIPSECによりセキュリティが確保される。

【0016】続いて、図14、図16、図19、図20を用いて上記ネットワーク接続装置1402及び1403におけるIPSEC処理の詳細を説明する。ここに図16は、AH(Authentication Header)フォーマット及び、ESP(Encapsulation Security Payload)ヘッダフォーマットの詳細図、図19は、送信側ネットワーク接続装置におけるIPSEC処理のフローチャート、図20は、受信側ネットワーク接続装置におけるIPSEC処理のフローチャートである。

【0017】尚、後述するSPD、SADはそれぞれのネットワーク接続装置内のデータ記憶部2103に記憶されている。ここで、図19、20におけるSはステップを意味する。

【0018】上記ネットワーク接続装置1402では、送信側のコンピュータ1401より送信されたIPパケットを受信すると、まずその送信先IPアドレスを読み出す(図19:S1901)。つづいて該送信先IPアドレスを基に上記ネットワーク接続装置1402に格納される上記SPD1701の送信先IPアドレス1702を検索し、対応するIPSECパケットを送信すべき先の通信端末のIPアドレス1705、IPSEC処理の有無1703及びSAの位置を示すアドレスポインタ1704を読み出す(図19:S1902)。

【0019】ここで、IPSEC処理を行わない設定、即ちIPSEC処理の有無1703が”無”の場合、上記受信したIPパケットをそのまま上記ネットワーク接続装置1403に送信する(図19:S1903のNo)。

【0020】IPSEC処理を行う設定、即ちIPSEC処理の有無1703が”有”の場合、更に上記SAの位置を示すアドレスポインタ1704を用いて上記SAD1801を検索し、該当するSAの内容を読み出す(図19:S1903のYes→S1905)。該SAは、上記IKEフェーズ2(1502)で確立されたSAである。次に、上記ネットワーク接続装置1402

は、上記SAの内容に従い、例えば認証アルゴリズムとしてHMAC-MA5を、暗号化アルゴリズムとしてDES-CBSを用いて上記IPパケットから認証／暗号化データを作成する(図19:S1905)。さらに、上記ネットワーク接続装置1402は、上記認証／暗号化データに、認証ヘッダAHまたは認証／暗号化ヘッダESPを追加し、IPSEC処理を施したIPパケット(IPSECパケット1503)とする(図19:S1906)。ここで、上記AH及びESPには上記IKEフェーズ2で確立したSAを構成する上記SPI1805が含まれる。続いて上記IPSECパケット1503は、インターネット1409を介して上記SPD1701のIPアドレス1705が示す上記ネットワーク接続装置1403に送信される。ここで、IPSECの処理には”トランスポートモード”と”トンネルモード”があり、上記説明はトンネルモードの説明であるが、例えば上記トランスポートモードを使用する場合には上記IPパケットの送信先IPアドレスは暗号化されない。又、上記トランスポートモード及びトンネルモードは適宜選択可能である。尚、上記AHフォーマット及びESPヘッダフォーマットの詳細を図16(a)、(b)に示す。

【0021】次に、上記ネットワーク接続装置1403は、受信したIPパケットがIPSECパケットであるかを判別する(図20:S2001)。

【0022】ここで、IPSECパケットでない場合、上記IPパケットはそのままLAN1408を介してコンピュータ1404に送信される(図20:S2001のNo)。

【0023】受信したIPパケットが、IPSECパケットである場合、以下の処理を行う(図20:S2001のYes)。即ち、まず上記IPSECパケット内の上記AHやESPヘッダを調べ、該AHやESPヘッダに含まれるSPIを読み出す(図20:S2002)。次に、上記ネットワーク接続装置1403に格納されるSADを上記SPIを用いて検索し、上記SPIに該当する、上記IKEフェーズ2で確立したSAの内容を読み出す(図20:S2003)。これにより、上述したIKEフェーズ2で確立した該当SAが読み出されることになる。ここで、S2002にて該当SPIが無い場合はユーザにその旨を表示して処理を終了する(図示せず)。

【0024】さらに、上記ネットワーク接続装置1403は、上記読み出したSAで指定された認証／暗号化アルゴリズム等を用いて、上記IPSECパケットの認証／暗号化データを認証／復号化する(図20:S2004)。又、必要に応じて上記SAのアドレス情報1804からSPD1701を検索し、送信元のIPアドレス及び、IPSEC処理の有無を確認し、元のIPパケットを生成する(図20:S2005→2006)。続い

て上記ネットワーク接続装置1403は生成した上記IPパケットをコンピュータ1404に送信する。

【0025】以上により、上記認証／復号化された上記IPSECパケットの認証／暗号化データは、IPパケットとしてLAN1408を介してコンピュータ1404に送信される。即ち、上記ネットワーク接続装置1402、1403間では、送信側のコンピュータ1401から上記コンピュータ1404に送信されるデータはIPSECにてセキュリティが確保される。

【0026】統いて、図21を用いて上記ネットワーク接続装置1402の構成の概略を説明する。尚、ネットワーク接続装置1403も同様の構成である。

【0027】上記ネットワーク接続装置1402及び1403は、一般的に図21に示すような構成を有する。即ち、処理部2101、一時データ記憶部2102、データ記憶部2103、システム制御部2104、ネットワーク制御部2106、回線制御部2107が内部バス或いはスイッチ2105にてそれぞれ接続されている。また、上記ネットワーク制御部2106は上記LAN1407に、上記回線制御部2107はインターネット1409とそれぞれ接続されている。

【0028】上述したSPD、SADは、フラッシュメモリ、ハードディスク、ROM等の不揮発性メモリで構成された上記データ記憶部2103に格納される。上記処理部2101は、上記ネットワーク接続装置1402の電源投入時に上記データ記憶部2103からシステム制御部2104を経由して、上記SPD、SADを読み出し、DRAM、SRAM等の揮発メモリで構成される上記一時データ記憶部2102に格納するかあるいは、必要なときに読み出し、一時データ記憶部2102に格納する。又、上記SPD、SADの更新は上記データ記憶部2103に格納されているSPD、SADに対して行なわれる。

【0029】LAN1407或いはインターネット1409からそれぞれネットワーク制御部2106、回線制御部2107を経由して受信した個々のIPパケット(IPSECパケット)は、上記処理部2101にて上述したIPSEC処理が行われる。即ち、上記処理部2101は、個々のIPSECパケットの上記AH、ESP情報を読み出し、上述した処理フローに従って上記一時データ記憶部2102に格納された必要なSPD、SADを検索してIPSECに関する認証／暗号化、認証／復号化を行なった後、送信先アドレスに送信する。また、その他の機能(ルーティング機能等)も上記処理部2101にて提供される。

【0030】ここで、個々のIPパケット処理時に、一時データ記憶部2102に格納されたSPD、SADを検索する理由は、上記一時データ記憶部2102がデータ記憶部2103に比べて高速にアクセス可能であり、上記IPSEC処理の高速化を図ることができるためである。

ある。

【0031】このように、一時データ記憶部2102に格納されたSPD、SADを参照して処理を進めるため、例えばSAに関するパラメータが変更された場合、変更後のSAパラメータが上記IPSECを用いた通信に反映されるのは、一般的に上記ネットワーク接続装置1402の電源投入時及び、リセット時等の起動時のみである。これは通常、ルータ等のネットワーク接続装置1402は連続通電され、常時運用されており、一時データ記憶部2102に格納されたSAに関するパラメータと変更されたパラメータとの整合をとる機構が必要なためと、現状のIPSECを用いた通信は、主に例えば本社と支社間等、決まったネットワーク接続装置間でのLAN間接続に用いられているため、上記データ記憶部2103に格納されるSPD、SAD、その他の設定パラメータについて、変更される機会が少ないと前提にしているためである。

【0032】

【発明が解決しようとする課題】上記のようなネットワーク層でのセキュリティプロトコルは、通信パケット全体に対してセキュリティを確保するため、アプリケーションごとにセキュリティを施す必要がなく、LAN間接続時のセキュリティ対策として利便性が高い。しかしながら、セキュリティに関する認証／暗号化等の処理は非常に計算量が多く、セキュリティの強度(即ち安全性)を高くすれば通信が漏洩する可能性が低くなるが、それだけ各コンピュータやネットワーク接続装置の負荷が高くなり、即ち、処理の遅延を招く。ここで、セキュリティの強度を下げれば当然通信が漏洩する可能性が高くなる。

【0033】従来技術では、上記のように相手先端末に対応してセキュリティ通信のレベルを設定しているため、例えば複数のユーザが使用する送信元端末から、暗号化の必要ないユーザが送信するデータにも、一定強度のセキュリティを付与する必要があった。このような通信は、各コンピュータやネットワーク接続装置の不必要的負荷を増大させ、即ち処理の遅延を招くに至っている。逆に、レベルの高いセキュリティを必要とするユーザが送信するデータであっても、それより低いレベルのセキュリティでしか送信できない難点があった。

【0034】また、従来のIPSEC機能を搭載したルータ等では、予め上述したように通信先のIPアドレスに対して使用するSAを対応付ける必要があり、さらにその対応付け手続きの困難性から、セキュリティ通信のレベルを柔軟に変更できないばかりでなく、専門知識のないユーザが各自で適宜セキュリティ通信のレベルを変えることが困難であった。しかしながらインターネットあるいは企業間のインターネットを介した電子メールの交換や、これらを利用した電子商取引が一般化しつつあるため、ネットワークに関する専門的な技術を持った保

守者がいる大企業等だけでなく、そのような専門的な技術者が期待できないS O H O (Small Office Home Office) や家庭においても使用できるような容易な設定方法が求められる。また、接続先や、電子商取引時のクレジット番号発信等、通信によって、セキュリティ通信のレベルを最適に変えたい場合があるが、従来の技術では、接続時のセキュリティ通信のレベルが最適かどうか分からぬという課題がある。本発明は、上記課題を解決するために提案するものであり、従来の利便性を損なうことなくデータ送信を行うユーザごとにセキュリティ通信のレベルを設定できると共に、ネットワークに関する専門知識がなくても容易に各種セキュリティ通信のための接続パラメータを変更でき、かつ直ちに該変更の有効性の確認、及び反映を行うことが可能であり、さらに、接続先との通信にどれ程のセキュリティ通信のレベルを設定すれば良いかを自動で決定できるセキュリティ通信方法を提供するものである。

【0035】

【課題を解決するための手段】本発明は、上記目的を達成するために以下の手段を備える。

【0036】すなわち、通信端末を使用するユーザの情報とセキュリティ種を対応付けた対応情報を記憶する記憶手段と、上記ユーザの情報に基づいて、上記対応情報からセキュリティ種を決定する上記セキュリティ種選択手段を備える。

【0037】さらに、上記セキュリティ種選択手段が、上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認する構成がある。

【0038】ユーザ毎にセキュリティ種を対応付けることにより、従来の利便性を損なうことなくデータ送信を行うユーザごとにセキュリティ通信のレベルを設定できる。又、上記対応情報の変更時に、上記変更後の情報に基づいた通信の確立を直ちに確認できることで、直ちに該変更の有効性の確認、及び反映を行うことが可能である。

【0039】又、通信端末にて動作するアプリケーションに入力されるインターネットアドレス情報と、セキュリティ種とを対応付けた対応情報を記憶する記憶手段と、上記インターネットアドレス情報に基づいて、上記対応情報からセキュリティ種を決定する上記セキュリティ種選択手段を備える。

【0040】さらに、上記通信端末を使用するユーザの情報とセキュリティ種とを対応付けた構成がある。

【0041】当該手段により、ユーザになじみの深いインターネットアドレス情報をセキュリティ種と対応付けることにより、ネットワークに関する専門知識がなくても容易に各種セキュリティ通信のための接続パラメータを変更できる。

【0042】又、通信装置が、セキュリティ種を所定のセキュリティ情報装置に問い合わせる問い合わせ手段

と、上記問い合わせに対応する回答に基づいて上記セキュリティ種を決定する上記セキュリティ種選択手段を備え、さらに上記セキュリティ情報装置が、通信装置の端末特定情報と、該通信装置との通信において推奨されるセキュリティ種とを対応付けた対応情報を記憶する記憶手段と、他の通信装置からの、上記通信装置について推奨されるセキュリティ種の問い合わせに対し、上記推奨されるセキュリティ種を選択する推奨セキュリティ種管理手段と、上記選択された推奨されるセキュリティ種を送信する送信手段を備える。

【0043】当該手段により、上記セキュリティ情報装置にセキュリティ種を問い合わせることにより、接続先との通信にどれ程のセキュリティ通信のレベルを設定すれば良いかを自動で決定できる。

【0044】尚、上記セキュリティ種が、セキュリティプロトコルである場合や、認証アルゴリズムや暗号化アルゴリズムを含む定義情報群である構成がある。

【0045】また、セキュリティ通信方法は、各通信装置又は通信端末に上述した手段をそれぞれ備えることにより実現する。

【0046】

【発明の実施の形態】以下、添付図面を参照して、主に従来例との違いについて本発明の実施の形態につき説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

【0047】〔実施の形態1〕始めに、図1、図2(a)、図2(b)、図4を参照しながら、実施の形態1におけるセキュリティ通信方法、通信システム及びその装置の概略について説明する。

【0048】図1は本発明に係るセキュリティ通信方法を用いたシステムの概略を示す図である。当該図1において、コンピュータ101はLAN107で他のコンピュータ105及びネットワーク接続装置102と接続されており、ネットワーク接続装置102を経由して、外部のインターネット109やインターネット等のWANに接続されている。このインターネット109には他のネットワーク接続装置103、LAN108が接続されており、該LANにはコンピュータ104、106が接続されている。ここで、上記ネットワーク接続装置102、103は、ルータ、ゲートウェイ、プロキシサーバ等のファイアウォールやVPN専用装置等である。さらに、上記コンピュータ101、105にはそれぞれユーザ認証装置110、111が接続されている。ここで、コンピュータ101他はパーソナルコンピュータ、ワープロステーション、サーバ、ノート型パソコン、IP電話、IPテレビ電話、IP携帯電話等の通信機能を持つ端末であればよい。以下、従来例と同様に、ネットワーク接続装置102、103間でIPSEC処理を行うものとして説明を行う。尚、IPSEC処理を行うのは前

記ネットワーク接続装置102、103に限定するものではなく、送信元コンピュータ101、送信先コンピュータ104間でも良く、また、コンピュータ102、ネットワーク接続装置103間でも良いのは従来例と同様である。又、図2(a)は本実施の形態1において用いられるユーザ毎のSPDであり、図2(b)はユーザ毎のSADの例である。上記ユーザ毎のSPD及びユーザ毎のSAD内容の詳細は後述する。

【0049】まず、図4の上記ネットワーク接続装置102(103も同様の構成である)の構成の概略図を用いて上記ネットワーク接続装置102、103の内部の処理を説明する。

【0050】本実施の形態における上記ネットワーク接続装置では、ユーザ毎に異なるセキュリティレベルを設定することを可能にするため、後述するユーザの設定及び送信先のIPアドレスの設定を行なう。このため、従来使用されているネットワーク接続装置のような本社と支社間等の決まったLANを接続している場合でも、例えばユーザの追加等、設定の更新が従来より多いことが予想される。このような更新の都度従来のような装置電源投入や装置リセット等を行なうと通信が短時間でもストップすることとなり、ユーザにとっては不便である。そこで、上記ネットワーク接続装置の内部処理を以下のようにすることにより、装置電源投入や装置リセット等を行なうことなく常時運用を実現する。

【0051】即ち、図4において、ネットワーク接続装置102、103は処理部401、一時データ記憶部402、データ記憶部403、システム制御部404、ネットワーク制御部406、回線制御部407を備え、それぞれ内部バス或いはスイッチ405にて接続されている。ここで、上記処理部401、一時データ記憶部402、システム制御部404は後述する処理におけるセキュリティ種選択手段408として機能する。

【0052】さらに、上記ユーザ毎のSPD201及び上記ユーザ毎のSAD207はフラッシュメモリ、ハードディスク、ROM等の不揮発メモリで構成されたデータ記憶部403に格納されている。また、上記ネットワーク接続装置102の電源投入時に上記処理部401は、上記データ記憶部403からシステム制御部404を経由して、上記ユーザ毎のSPD201、ユーザ毎のSAD207を読み出し、DRAM、SRAM等の揮発メモリで構成される上記一時データ記憶部402に格納する。以後、上記処理部401では、上記一時データ記憶部402に格納された上記ユーザ毎のSPD201、ユーザ毎のSAD207を用いてIPSEC処理が行なわれる。又、設定の変更に伴う上記ユーザ毎のSPD201、ユーザ毎のSAD207の更新はデータ記憶部403に格納されているユーザ毎のSPD201、ユーザ毎のSAD207に対して行なわれる。ここまで処理は、上記ユーザ毎のSPD201及び、ユーザ毎のSA

D207の構造を除き、前記従来技術と同様である。

【0053】ここで、従来技術では、一時データ記憶部に格納されたSPD、SADを参照してIPSEC処理を進め、再度データ記憶部からSPD、SADが読みだされるのは装置電源投入や装置リセット等を行なった後の装置起動時のみであった。このため、SPD、SADが変更された場合、その更新されたSAがIPSEC処理に反映されるのは、同じく装置電源投入時及び装置リセット時等の装置起動後であった。

【0054】しかし、本実施の形態では、上記データ記憶部403の上記SPD、SADが設定の変更等により更新された場合には以下の処理を行なう。即ち、上記処理部401は、上記一時データ記憶部402に格納されているSPD、SADを用いて通信処理を行なっている場合は該処理中の処理が終わり次第通信を中断するとともに、更新されたSPD、SADをデータ記憶部403から読み出し、上記一時データ記憶部402に格納された該当するSPD、SADに上書きする。ここで、上書きするのは上記更新されたSPD、SADのみであり、ユーザ毎のSPDのうち、更新されていないものについては更新を行わない。これにより、更新に関係しないSPD、SADを用いて通信を行なっているユーザのIPSEC通信には影響を及ぼさない。

【0055】次に、該格納されたSPD、SADを用いて上述したIKEフェーズ2を用いてSAを再確立し、新たに確立された該SAを用いてIPSEC処理を再開する。

【0056】上述したSPD、SADの更新処理を行なうことにより、セキュリティ通信のレベルを変更した場合でも、装置を再度起動する必要がなく、直ちに更新の有効性の確認、即ちIKEフェーズ2を用いたSAの再確立、及び更新の反映を行うことが可能である。

【0057】尚、IPSEC通信中のSAの再確立については、通信を中断して即時再確立を行なう方法や、処理中のIPSEC通信が終了してから再確立を行う方法を予め選択できるとともに、処理するパケットの種類に応じて上記再確立の方法を選択できるものとする。

【0058】次に、セキュリティ通信を始めるにあたり予め上記ネットワーク接続装置102において、図2に示すユーザ毎のSPD、ユーザ毎のSAD等の定義情報群を設定する手順の詳細を説明する。

【0059】即ち、まず上記ネットワーク接続装置102の管理者は、当該ネットワーク接続装置102の上記処理部401に対し、上記コンピュータ101、105を使用するユーザ毎に、各送信先IPアドレスと、通信する際のIPSEC処理を行なうか否かの設定を行ない、ユーザ毎のSPD(SPD-1～SPD-N)設定を行う。尚、ユーザを識別する方法については後述する。ここで、上記各送信先IPアドレスが、例えば上記コンピュータ104、106のIPアドレスを指すこと

は、従来例の場合と同様である。又、該設定は上記コンピュータ101、105等の例えはWEBブラウザ等より行うか又は、直接ネットワーク接続装置102にて行うことができる。又、上記各送信先IPアドレスは従来技術と同様範囲指定が可能である。

【0060】次に、IPSEC処理を行なう場合には該IPSEC処理に使用するSAの内容である認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含むユーザ毎の一連の定義情報群SAD(SAD-1～SAD-N)の設定も行なう。上記設定により、図2(a)に示すユーザ毎のSPD201が上記ネットワーク接続装置102のデータ記憶部403に複数登録され、さらに、上記SAの内容である認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含む一連の定義情報群がユーザ毎のSAD207として登録される。上記登録されたSAD207が含むSAは後述するIKEフェーズ2にてネットワーク接続装置103に提案される。

【0061】ここで、図2(a)に示すユーザ毎のSPD201は、前記従来技術におけるSPD1701と同様、送信先アドレス202、IPSEC処理の有無203、SAの位置を示すアドレスポインタ204、送信先IPアドレス202にデータを送信する場合に、IPSECパケットを送信すべき先の通信端末のIPアドレス206を含むが、さらにユーザ名205によって区別されている点で従来技術と異なる。尚、図2(a)にはユーザ毎にSPDを設ける例を示したが、1つのSPD内に個々のユーザを識別する項目を設けることによりユーザ毎のSAを指定してもよい。

【0062】同様に、図2(b)に示すユーザ毎のSAD207は、図18に示す従来技術におけるSAD1801と同様の構成を有し、1つのSADに複数のSAを含む。例えば、SAD-1にはSA-11からSA-1M(211)を含み、同様に、SAD-NにはSA-N1からSA-NMを含む。また、アドレス情報209、インデックス情報であるSPI210、セキュリティパラメータであるSAP212を有する。上記アドレス情報209には送信先IPアドレス、送信先ポート番号、送信元IPアドレス、送信元ポート番号、プロトコル番号等が含まれる点も、従来技術と同様である。但し、ユーザ名208によって区別されている点で従来技術と異なる。尚、図2(b)にはユーザ毎にSADを設ける例を示したが、1つのSAD内に個々のユーザを識別する項目を設けることによりユーザ毎のSAを管理してもよい。

【0063】上記設定が終了すると、上記ネットワーク接続装置102は、後述するユーザ情報を元に、上記設定の有効性を確認するために、前記従来技術と同様IKEフェーズ1及びフェーズ2を用いて、上記ネットワーク接続装置103と通信を行ない、上記設定された内容

に基づいてIPSEC通信が可能であるかを確認とともに、通信が可能であればSAを確立する。尚、前記SAの確立は、上記設定の終了時に必ずしも行う必要はない、例えばコンピュータ101とコンピュータ104が上記ネットワーク接続装置102及びネットワーク接続装置103を介して通信を開始する場合に行なってよい。

【0064】また、上記ネットワーク接続装置103に対しても、上記ネットワーク接続装置102に対して行なった場合と同様、上記コンピュータ104、106にユーザ認証装置を接続する等して、当該コンピュータ104、106を使用するユーザ毎に、各送信先IPアドレスに関する設定を行なってよい。

【0065】続いて、上記コンピュータ101を使用するユーザの識別方法について説明する。

【0066】上記コンピュータ101を使用するユーザは、該コンピュータ101の使用時に上記ユーザを特定することができる固有番号を記憶しているICカードを上記ユーザ認証装置110に通して入力する。次に、該ユーザ認証装置110より上記固有番号に対応するパスワードを入力する。上記ユーザ認証装置110にて入力されたICカードの固有番号と上記パスワードが、あらかじめ設定されているものと一致すれば上記ユーザは認証され、上記コンピュータ101を使用可能となる。また上記ユーザの認証により得られたユーザ名が上記コンピュータ101に記憶される。

【0067】尚、上記ユーザの認証はICカードである必要は無く、例えば磁気カード、ワンタイムパスワード、指紋、掌形、掌皺、筆跡、虹彩、顔面形状、声紋、DNA等で個人を識別する装置でもよく、さらには、上記ユーザ認証装置を設けず、上記コンピュータ101へのユーザ名とパスワードの入力によって上記認証を行なってよい。さらに、上記あらかじめ設定された固有番号及びパスワードの記憶場所は、上記コンピュータ101である必要は無く、例えば固有番号及びパスワードを一元管理するコンピュータを別途設け、ユーザの認証時に上記コンピュータ101から上記一元管理するコンピュータに問い合わせを行なってよい。

【0068】次に、図1、図2、図3を用いて、上記コンピュータ101がインターネット109を介して接続される上記コンピュータ104と通信を行なう場合の処理の詳細を説明する。以下の処理は、上述した図4におけるセキュリティ種選択手段408にて実行される。

【0069】尚、上記IPSEC通信に使用されるSAが確立された後、送信側のコンピュータ101から上記コンピュータ104に送信されるデータは、上記コンピュータ101にてIPヘッダを附加され、IPパケットとしてLAN107を介してネットワーク接続装置102に送られる点は前記従来技術と同様である。但し、本実施の形態においては、加えて上記ユーザ認証にて得ら

れたユーザ名を上記IPヘッダのオプション部に挿入する処理が行なわれている。上記オプション部は、上記IPヘッダ中でユーザ（設計者）が任意に使用できるデータエリアである。

【0070】ネットワーク接続装置102では、送信側のコンピュータ101より送信されたIPパケットを受信すると、まず、該IPパケットに含まれるユーザ名及び送信先IPアドレスを読み出す（図3：S301）。つづいて複数のユーザ毎のSPD201より上記ユーザ名に対応するSPDを選択し、さらに該ユーザ名に対応するSPDから、上記送信先IPアドレスをもとに送信先IPアドレス202を検索する（図3：S302）。また、対応するIPSEC処理203の有無を確認する。

【0071】ここで、上記IPSEC処理203が”無”、即ちIPSEC処理を行なわない設定の場合、後述するIPSEC処理は行なわずに上記受信したIPパケットをそのまま上記ネットワーク接続装置103に送信する（図3：S303のNo）。

【0072】上記IPSEC処理203が”有”、即ちIPSEC処理を行う設定である場合、さらに、対応する上記IPSECパケットを送信すべき先の通信端末のIPアドレス206及びSAの位置を示すアドレスポインタ204を読み出すと共に、該アドレスポインタ204に基づいて該当するSAを読み出す（図3：S304）。尚、当該SAは、上記IKEフェーズ2で確立されたSAである点は、従来技術と同様である。

【0073】次に、上記ネットワーク接続装置102は、上記SAの内容に従い、所定の認証アルゴリズム及び暗号化アルゴリズムを用いて上記IPパケットから認証／暗号化データを作成する（図3：S305）。さらに、上記ネットワーク接続装置102は、上記認証／暗号化データに、認証ヘッダであるAHまたは認証／暗号化ヘッダであるESPを追加し、次いで、送信先アドレスを上記IPSECパケットを送信すべき先の通信端末のIPアドレス206としてインターネット109を介して上記ネットワーク接続装置103に送信する（図3：S306）。

【0074】以降、上記ネットワーク接続装置103が、受信したIPパケットがIPSECパケットであるかを判別し、元のIPパケットを生成するまでの処理は前記従来技術と同様である。

【0075】以上のように、予めユーザ毎にSPDを設け、さらに、各通信端末におけるユーザ認証の情報を用いてセキュリティ通信の内容を示すSAを決定するため、従来の利便性を損なうことなくユーザに応じて最適なセキュリティ通信のレベルを設定することが可能となる。

【0076】尚、上述した実施の形態1では、ネットワーク接続装置にIPSEC機能を搭載しているが、当

然、コンピュータ101や104等にIPSEC機能を搭載しセキュリティ通信を行っても問題ない。

【0077】尚、SAが確立した状態で、ユーザ名に対応するSPDを検索した場合で、該当するSPDが無い場合、及び、SPDに該当IPアドレスが無い場合（図示せず）、ユーザにその旨を表示し、セキュリティ処理を施さずIPパケットを送出しても良いし、また、送信を行わないといったことも可能である。また、ユーザに送信するかどうか問い合わせるといった対応を行ってもよい。尚、SPDでIPSEC処理を行わない設定になっていた場合は、そのままIPSEC処理を行わず送信先IPアドレスにIPパケットを送出する。

【0078】さらに、本実施の形態では、セキュリティ通信のプロトコルをIPSECに限定しているが、ネットワーク接続装置が複数のセキュリティ通信のプロトコルを搭載している場合には、上記ユーザ情報と上記セキュリティ通信のプロトコルを対応付けることにより、ユーザによってセキュリティ通信のプロトコルを使い分けることが可能になる。上記セキュリティ通信のプロトコルを使い分けることにより、更に多種多様なセキュリティ通信を行なうことが出来る。

【0079】さらに、本実施の形態ではIPSECを用いて各ユーザに対応するSPDを指定しているが、IPSEC以外のプロトコルを用いる場合についても同様であり、ユーザ認証情報から対応するSPDもしくはSPDに相当するデータベースを参照して、SAもしくはSAに相当する情報を指定することにより、認証アルゴリズム、暗号化アルゴリズム等の一連の定義情報群を指定することが出来る。当然、用いるプロトコルの種類によってはSPDを参照せずに直接SAを指定してもよい。

【0080】また、ユーザ数が多数の場合等にはユーザ毎にSPDを作成せず、各ユーザが所属するグループを作成し、該グループごとにセキュリティ通信のレベルを変更してもよい。この場合には、ユーザ認証時にグループ情報も併せて管理し、該グループ情報を以て上記SPDを参照する。

【0081】尚、本実施の形態では、ユーザ認証にて得られたユーザ名をIPヘッダのオプション部に挿入することにより、各IPパケットとユーザ名を対応付けているが、例えばユーザ認証時に該認証内容を各コンピュータがネットワーク接続装置に通知し、該ネットワーク接続装置にて各ユーザ名とコンピュータをそれぞれ対応づけるデータベースを持つことにより各IPパケットとユーザ名の対応付けを行ってもよい。

【0082】〔実施の形態2〕次に、図5、図6を参照しながら、実施の形態2におけるアプリケーション層のアドレス情報をSAに対応づける方法について説明する。ここでアプリケーション層とは、OSI参照モデルの第7層を指し、主に通信処理が関係するアプリケーションを意味する。ここで、アプリケーション層のインタ

一ネットアドレス情報はホスト名、あるいはホスト名と接続プロトコルを組み合わせたURL (Uniform Resource Locator) 表記を含むものとする。また、後述するネットワーク接続装置は上記実施の形態1で示した場合と同様、セキュリティ通信のレベルを変更した場合でも、装置を再度起動しなおすことなく変更を反映できるものである。

【0083】図5に示すインターネットアドレスを用いたSPD501は、インターネットアドレス502、送信先IPアドレス503、IPSEC処理の有無504、SAの位置を示すアドレスポインタ505、送信先IPアドレス503にデータを送信する場合に、IPSECパケットを送信すべき先の通信端末のIPアドレス506を備える。上記インターネットアドレス502を備える点を除いては従来技術におけるSPD1701と同様である。また、上記アドレスポインタ505の示すSAが含まれるSADの構成も、従来技術のSAD1801と同様である。さらに、上記インターネットアドレス502は具体的には例えば"http://abc.def.com"といったURLや"abc@def.com"といった電子メールアドレス、同様に電子メールの送受信に使用されるPOPサーバ(Post Office Protocol サーバ)、SMTPサーバ(Simple Mail Transfer Protocol サーバ)等のアドレスが格納される。

【0084】まず始めに図6を用いて本実施の形態2における、アプリケーション層のアドレス情報をSAに対応づける具体的な操作の例を説明する。図6はIPSEC機能を搭載したネットワーク接続装置の設定を行うコンピュータ等の通信端末装置の概略図である。

【0085】図6において、通信端末装置本体608は、制御手段609、ディスプレイ601、ネットワーク接続装置管理手段610、入力手段611、指示入力手段612を備える。また、後述する各ソフトウェアは上記制御手段609又は該上記制御手段609を構成する上記ネットワーク接続装置管理手段にて実行される。また、上記通信端末装置本体608を使用するユーザに対する情報の表示等は、必要に応じて上記各ソフトウェアの表示機能により上記ディスプレイ601に表示される。

【0086】まず、上記通信端末装置本体608の上記制御手段609にて、アプリケーション層のアドレス情報となるURL603を表示するアプリケーションソフトウェアであるWEB閲覧ソフトウェア602等を実行する。

【0087】さらに、上記ネットワーク接続装置管理手段610にて、ネットワーク接続装置管理ソフトウェア605を実行する。該ネットワーク接続装置管理ソフトウェア605は、パラメータ設定用ウインドウ606及び設定ボタン607を表示する機能を有し、上記パラメータ設定用ウインドウ606には上記ネットワーク接続

装置がサポートする複数のSAが表示されている。尚、上記複数のSAは、認証アルゴリズム、暗号化アルゴリズム等が異なり、この違いによりセキュリティ通信のレベルが異なるものである。又、上記ディスプレイ601は上記ネットワーク接続装置に直接接続され、該ネットワーク接続装置が上記制御手段609及びネットワーク接続装置管理手段610の機能を提供してもよいが、ネットワーク接続装置とネットワークを介して接続されているコンピュータ(例えばコンピュータ101)にて上記制御手段609及びネットワーク接続装置管理手段610の機能を提供してもよい。この場合には、上記操作は上記コンピュータによって行われ、通信によって上記操作の変更が上記ネットワーク接続装置に反映される。

【0088】上記ネットワーク接続装置の設定を行うユーザは、上記通信端末装置本体608にて、ディスプレイ601に表示されているアドレス情報である上記URL603等を指示入力手段612を用いてドラッグし、上記パラメータ設定用ウインドウ606に表示されている複数のSAの内の希望する任意の一つにドロップする。上記指示入力手段612とは、例えばコンピュータにて一般的に使用されるマウス、トラックボール、ジョイスティック、タッチペン、指等のポインタ指示手段であり、該指示入力手段612が指示するディスプレイ601上の位置がポインタ604として表示される。この操作により上記アプリケーション層のアドレス情報をSAに対応づけることができる。続いて上記設定ボタン607をクリックすることにより、上記ネットワーク接続装置にて後述する設定処理が行われる。尚、設定ボタン607をクリックした場合、IPSEC通信の途中であっても、当該通信を中断して、直ちに当該設定更新処理を行うか、当該通信が終了してから直ちに当該設定更新処理を行うかは設定等で選択できるものとする。また、通信を行う場合に初めて当該設定変更があった通信先とセキュリティ通信のための接続を行うか、直ちに前記接続を行うかについても設定等で選択が可能であるものとする。

【0089】次に、図4、図5、図7を用いて、上記ユーザによる操作が終了した後の上記ネットワーク接続装置にて行われる設定処理を説明する。まず、ネットワーク接続装置の設定を行うユーザが上述したように上記アプリケーション層のアドレス情報をSAに対応づけた後、上記ネットワーク接続装置の処理部401はデータ記憶部403に格納されるSPD501のインターネットアドレス502にアプリケーション層のアドレス情報を格納する(図7:S701～S702)。

【0090】次に上記処理部401はDNSサーバ(Domain Name System サーバ)を用いて上記アドレス情報をIPアドレスに変換する(図7:S703)。ここに、DNSサーバとは、インターネット接続環境があれば一般的に使用できるサービスで、上記アドレス情報で

ある例えは”abc.def.com”といった文字列を用いて問い合わせることにより、上記”abc.def.com”に対応するIPアドレスを回答するサーバである。次に、上記処理部401は、上記変換したIPアドレスを上記SPD501の送信先IPアドレス503に格納し、さらに上記データ記憶部403に格納されるSAD1801を構成するアドレス情報1804に必要な、送信先IPアドレス、送信先ポート番号、送信元IPアドレス、送信元ポート番号、プロトコル番号等をそれぞれ上記SADに格納する（図7：S704）。ここで、上記送信先、送信元ポート番号及びプロトコル番号は、例えば上記アドレス情報の一部である”http”により判断される。

【0091】上記SPD501及びSAD1801に必要な情報がそろった後、上記ネットワーク接続装置のセキュリティ選択手段408は、上記設定による接続の確認を行うかをユーザに問い合わせる（図7：S705）。尚、ユーザへの問い合わせは、別途設定で自動的に行うかどうかを設定してもよく、また、接続の確認を行う設定アイコン又はボタンを設けて、その設定アイコンまたはボタンが押されたら接続の確認を行うようにしてもよい。

【0092】接続の確認を行う場合は、上記送信先IPアドレスに対して従来技術同様IKEフェーズ1、フェーズ2及び、新たに設定された上記SPD501及びSAD1801の情報を用いて接続確認を行い、該結果をユーザに通知する（図7：S705のYes→S707）。以上の処理により、アプリケーション層のアドレス情報のSAへの対応付けが完了する。設定後は、上記新たに設定されたSPD501及びSAD1801を用いてセキュリティ通信が行われる。

【0093】尚、上記接続確認は、特にユーザに問い合わせる必要はなく、自動で確認を行うようにしてもよい。又、後述するセキュリティ情報装置を導入することで上記IPSEC機能を搭載した通信端末のIPアドレスの入力を自動で行うことも可能となる。

【0094】このように、普段よく使用するアプリケーションで指定するアドレス情報を用いてSAの設定を行うことにより、専門知識のないユーザでもSAの指定を容易に行なうことが出来る。

【0095】さらに、上記パラメータ設定用ウインドウ606のSAの表示を、例えば”セキュリティ高”、“セキュリティ中”、“セキュリティ低”、“セキュリティ無し”といった表示にすることにより、ユーザによるアドレス情報のSAへの対応付けをより分かりやすくすることが出来る。

【0096】尚、本実施の形態2ではIPSECを用いた場合のアドレス情報のSAへの対応付け例を示しているが、IPSEC以外のプロトコルを用いる場合についても同様である。

【0097】当然、上記実施の形態1にて実施されるユ

ーザ毎のセキュリティ通信と同時に実施しても何ら問題ない。この場合のSPDの例を図8のSPD801に示す。

【0098】〔実施の形態3〕次に、図9、図10、図11、図12、図13を参照しながら、実施の形態3におけるセキュリティ情報装置の機能について説明する。図9に示す各種機器等101～111は図1に示したものと同様であるが、さらにネットワーク接続装置902を介してセキュリティ情報装置901がインターネット109に接続されている。ここで、上記ネットワーク接続装置902は特にIPSEC機能を搭載している必要はなく、上記セキュリティ情報装置901に対する外部からの不正なアクセスを防ぐものであればよい。

【0099】上記セキュリティ情報装置901は、図13(a)に示される構成を有する。即ち、推奨SA管理手段1301、記憶手段1302を具備し、上記推奨SA管理手段1301は、送受信手段1304を介して上記ネットワーク接続装置902と接続されている。また、図11に示す推奨するSAを検索するための第1のデータベース1101及び、図12に示す推奨するSAを検索するための第2のデータベース1201が、上記記憶手段1302に格納されており、必要に応じて上記推奨SA管理手段が読み出し可能である。

【0100】また、ネットワーク接続装置102、103は、図13(b)に示すように送受信手段1308、記憶手段1309、制御手段1305を備え、該制御手段1305はさらに問い合わせ手段1306及び問い合わせ回答手段1307を備える。

【0101】次に、コンピュータ104は、図13(c)に示すように送受信手段1312問い合わせ回答手段1311を備える。尚、各手段の機能は適宜説明する。

【0102】上記第1のデータベースは、送信先IPアドレス1102、IPSECパケットを送信すべき先の通信端末のIPアドレス1103、IPSEC処理の有無1104、SAの位置を表すアドレスポインタ1105より構成される。ここで、上記送信先IPアドレス1102及びIPSECパケットを送信すべき先の通信端末のIPアドレス1103は、IPアドレスの範囲を登録することも可能である。また、上記IPSECパケットを送信すべき先の通信端末のIPアドレス1103は、IPアドレス1102に対してIPSEC処理を行う、IPSEC機能を搭載した通信端末のIPアドレスである。

【0103】更に図12は、推奨するSAを格納する第2のデータベース1201であり、複数の推奨SAが格納されている。該推奨SAとは、送信先であるIPSEC機能を搭載した通信端末が推奨するSAや、第3者機関が規定したSAであり、送信先の提供するサービスによってセキュリティ通信のレベルが異なる。尚、図10

は、理解に供するため、図9から説明に不必要的機器を省略したものである。本実施の形態3では、まず、図9において、ネットワーク接続装置102が、IPSEC通信を行おうとするネットワーク接続装置103との間でSAの確立を行う前に、セキュリティ情報装置901に上記IPSEC通信にふさわしい推奨SAを問い合わせる。上記ネットワーク接続装置102とネットワーク接続装置103との間でSAの確立を行うのは、例えば上記ネットワーク接続装置102及びネットワーク接続装置103の初期設定時や、コンピュータ101とコンピュータ104が上記ネットワーク接続装置102及びネットワーク接続装置103を介して通信を開始する場合等である。尚、推奨SAでSAの確立を図ったにもかかわらず、希望する推奨SAでSAが確立できない場合、送信を中止する、あるいはユーザに問い合わせる、そのまま推奨SA以外のSAでSA確立を行い、IPSEC通信を行う等の方法が考えられる。

【0104】ここでコンピュータ101とコンピュータ104が上記ネットワーク接続装置102及びネットワーク接続装置103を介して通信を開始する場合の上記推奨SAの問い合わせを想定すると以下のようになる。

【0105】即ち、ネットワーク接続装置102が上記コンピュータ101より上記コンピュータ104に送信するIPパケットを上記送受信手段1308を介して受信すると、上記制御手段1305は上記ネットワーク接続装置102の上記記憶手段1309に格納されるSPDを読み出す。

【0106】ここで該SPDに上記コンピュータ104の情報がない場合、上記ネットワーク接続装置102は、上記問い合わせ手段1306により、セキュリティ情報装置901に上記IPSEC通信にふさわしい推奨SAを問い合わせる(図10S1001)。尚、上記セキュリティ情報装置901のアドレスは予め上記ネットワーク接続装置102の記憶手段1309に格納されているものとする。

【0107】上記推奨SAの問い合わせにあたり、上記ネットワーク接続装置102は、送信先のコンピュータ104のIPアドレスを上記セキュリティ情報装置901に送信する。上記送受信手段1304を介して上記コンピュータ104のIPアドレスを受信した上記セキュリティ情報装置901の推奨SA管理手段1301は、上記コンピュータ104のIPアドレスを基に、上記記憶手段1302に格納されている上記第1のデータベース1101の送信先IPアドレス1102を検索し、対応する上記IPSECパケットを送信すべき先の通信端末のIPアドレス1103、IPSEC処理の有無1104及び、SAの位置を表すアドレスポインタ1105を得る。

【0108】さらに、上記推奨SA管理手段1301は、上記アドレスポインタ1105を用いて上記記憶手

段1302に格納されている第2のデータベース1201より推奨SAを得、該推奨するSAを、上記送受信手段1304を介してIPSECパケットを送信すべき先の通信端末のIPアドレス1103、IPSEC処理の有無1104と共に上記ネットワーク接続装置102に返送する(図10S1002)。

【0109】ここで、上記IPSECパケットを送信すべき先の通信端末のIPアドレス1103には、予め登録された上記ネットワーク接続装置103のIPアドレスが記憶されている。尚、返送する推奨SAの数は複数であっても構わない。

【0110】次に、上記推奨SA、上記IPSECパケットを送信すべき先の通信端末のIPアドレス1103及びIPSEC処理の有無1104を受信したネットワーク接続装置102の上記制御手段1305は、上記受信したIPSECパケットを送信すべき先の通信端末のIPアドレス1103に基づいてネットワーク接続装置103との間で、従来技術で説明したSAの確立を行い、IKEフェーズ2におけるSAの候補として、推奨SAを提案する(図10S1003)。

【0111】ネットワーク接続装置103は受け取った推奨SAでのIPSEC通信が可能な場合は、ネットワーク接続装置102に該推奨SAを返送し、SAの確立が行われる(図10S1004)。

【0112】従って、上記ネットワーク接続装置102がセキュリティ情報装置901に推奨SAを問い合わせることによって、相手先と安全に通信が可能なSAを知ることができ、該推奨SAによるIPSEC通信が可能となる。

【0113】ここで、上記ネットワーク通信装置102が上記IPSEC通信にふさわしい推奨SAの問い合わせを行った場合で、上記セキュリティ情報装置901の上記第1のデータベース中に該当IPアドレスの登録がない場合が考えられる(図10S1001)。

【0114】このような場合、上記セキュリティ情報装置901の上記推奨SA管理手段1301は、該当するコンピュータ104に、セキュリティ通信に必要なSAの候補を問い合わせる(図10S1005)。

【0115】問い合わせを受けた上記コンピュータ104は、問い合わせ回答手段1311により、該コンピュータ104に予め登録されている、IPSEC機能を搭載したネットワーク接続装置103のIPアドレスを上記セキュリティ情報装置901に返送する(図10S1006)。

【0116】上記IPSEC機能を搭載したネットワーク接続装置103のIPアドレスを受信した上記セキュリティ情報装置901の推奨SA管理手段1301は、上記ネットワーク接続装置103に対しSAの候補を問い合わせる(図10S1007)。問い合わせを受けた上記ネットワーク接続装置103の制御手段1305

は、該ネットワーク接続装置103の記憶手段1309に格納されているSAの候補を、問い合わせ回答手段1307により上記認証サーバ901に送信する(図10S1008)。

【0117】上記SAの候補を受信したセキュリティ情報装置901の推奨SA管理手段1301は、上記第2のデータベース1201に上記候補のSAを登録するとともに、上記第1のデータベース1101に上記ネットワーク通信装置102より問い合わせに使用されたIPアドレスと上記候補のSAの位置を表すアドレスポインタ1105、IPSECパケットを送信すべき先の通信末端のIPアドレス1103、IPSEC処理の有無1104を登録する。さらに、上記推奨するSAを、上記送受信手段1304を介してIPSECパケットを送信すべき先の通信末端のIPアドレス1103、IPSEC処理の有無1104と共に上記ネットワーク接続装置102に返送する(図10S1002)。

【0118】但し、問い合わせを受けた上記コンピュータ104に上記ネットワーク接続装置103のIPアドレスが登録されていない場合、やIPSEC機能を搭載した通信末端等が無い場合、或いは上記問い合わせ回答手段1311を備えない場合、その旨を上記セキュリティ情報装置901に返答するか若しくは返答を行わない。該返答を受けた若しくは返答を受けることが出来なかつた上記セキュリティ情報装置901は、上記旨を上記ネットワーク接続装置102に通知すると共に、上記第1のデータベース1101の送信先IPアドレス1102に上記コンピュータ104のIPアドレスを登録し、さらにIPSEC処理の有無1104を”無し”とする。このような場合には、上記ネットワーク接続装置102の制御手段1305は、上記コンピュータ101のユーザにセキュリティ通信を行えない旨を通知し、又は通信を行わないといった対応を行ってもよい。

【0119】尚、前記従来技術で述べたように、IKEフェーズ2では、双方通信の場合は独立した2つのSAが設定される。よって、ネットワーク接続装置102の要請によりIKEフェーズ2によるSAの確立を行う際に、上記ネットワーク接続装置103の制御手段1305は、上記セキュリティ情報装置901に対して上記ネットワーク接続装置102の推奨SAの問い合わせを行ってもよい(図10S1009)。

【0120】上記セキュリティ情報装置901の上記第1のデータベース1101に上記ネットワーク接続装置102の推奨SAが登録されていない場合、上記セキュリティ情報装置901の推奨SA管理手段1301が、上記ネットワーク接続装置102にSAの候補を問い合わせるといった処理が行われる(図10S1010～S1011)。つづいて、上記問い合わせに対応する回答が上記ネットワーク接続装置103に通知される(図10S1012)。この手順は上記処理S1001～S1

002、S1007～S1008と同様であるため詳細は省略する。

【0121】この様に、セキュリティ情報装置を設けることにより、ユーザが通信先のセキュリティ通信のレベルを考える必要がなく、適切なSAを設定可能となる。さらに、例えば上記セキュリティ情報装置を第三者機関が管理することにより、通信先アドレスによって、通信先が提供するサービス内容によってセキュリティ通信のレベルを最適にすることが可能となる。また、セキュリティ情報装置が、自動的に該当する通信端末にSAの候補を問い合わせて、該問い合わせの内容を収集することにより推奨SAを一元管理することが可能となり、各IPSEC機能を搭載した通信端末は、上記セキュリティ情報装置に問い合わせを行うのみで推奨SAの候補を得ることが可能となる。この様なシステムは、例えば複数の会社をIPSEC機能を搭載したルータ等で接続する場合等、IPSEC通信を適用する規模が大きい場合には特に通信端末に対する設定が簡単に行え、管理者及びユーザの負担軽減等に有効である。

【0122】尚、上記セキュリティ情報装置が格納するデータベースを2つに分けているが、特に分ける必要はなく、上記機能が実現できれば1つのデータベースにしてもよい。さらに、上述した項目に限らず、その他SAに必要な情報を格納することができる。

【0123】更にセキュリティ情報装置がRADUIS(Remote Authentication Dial-InUser Service)サーバを兼ねてもよく、IKEで交換される鍵情報の管理や、SAと対応するSPI情報の管理を同時にを行い、これら情報を提供してもよい。

【0124】また、各コンピュータがIPSEC機能を搭載する場合も上記ネットワーク接続装置と同様、セキュリティ情報装置に問い合わせを行うことができる。

【0125】又、上記送信先IPアドレスやIPSECパケットを送信すべき先の通信末端のIPアドレスは、IPアドレスを用いているが、特にIPアドレスに限定するものではなく、送信先通信末端(コンピュータ)を特定する末端特定情報であれば良く、例えばコンピュータ名やMACアドレス(Media Access Control Address)、電話番号等でもよい。

【0126】さらに、実施の形態3は、上記実施の形態1と組み合わせて使用することが可能であり、この場合には上記制御手段1305及び記憶手段1309がセキュリティ種選択手段408となり、送受信制御部1308が、ネットワーク制御部406及び回線制御部407となる。

【図面の簡単な説明】

【図1】本発明に係るセキュリティ通信方法を用いたシステムの概略を示す図。

【図2】実施の形態1におけるユーザ毎のSPD及びユーザ毎のSADの例。

【図3】実施の形態1におけるネットワーク処理装置のIPSEC処理のフローチャート。

【図4】実施の形態1におけるネットワーク接続装置の構成の概略図。

【図5】実施の形態2におけるインターネットアドレスを用いたSPDの例。

【図6】実施の形態2におけるIPSEC機能を搭載したネットワーク接続装置の設定を行うコンピュータ等の通信端末装置の概略図。

【図7】実施の形態2におけるネットワーク接続装置の設定確認処理のフローチャート。

【図8】実施の形態2におけるユーザ毎のインターネットアドレスを用いたSPDの例。

【図9】実施の形態3におけるセキュリティ情報装置を用いたシステムの概略を示す図。

【図10】セキュリティ情報装置を用いたシステムの処理を説明するための簡易図。

【図11】セキュリティ情報装置における第1のデータベースの例。

【図12】セキュリティ情報装置における第2のデータベースの例。

【図13】実施の形態3における各装置の概略を示すロック図。

【図14】IPSEC機能を搭載したルータを使用して

VPNネットワークを構成したネットワークシステムの概略図。

【図15】IPSEC機能を搭載したネットワーク接続装置間でのセキュリティ通信の接続手順を表した図。

【図16】AHフォーマット、ESPヘッダフォーマットの詳細図。

【図17】従来技術におけるIPSECの処理方針を決めるデータベースであるSPD(Security Policy Database)の例。

【図18】従来技術におけるSAデータベースであるSAD(Security Association Database)の例。

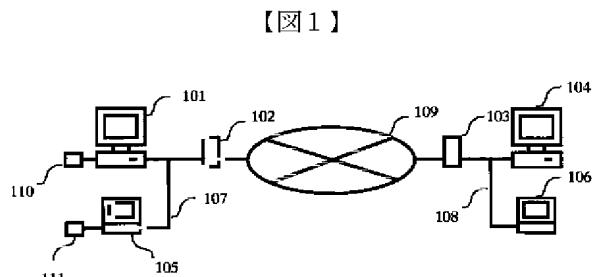
【図19】従来技術における送信側ネットワーク接続装置のIPSEC処理のフローチャート。

【図20】従来技術における受信側ネットワーク接続装置のIPSEC処理のフローチャート。

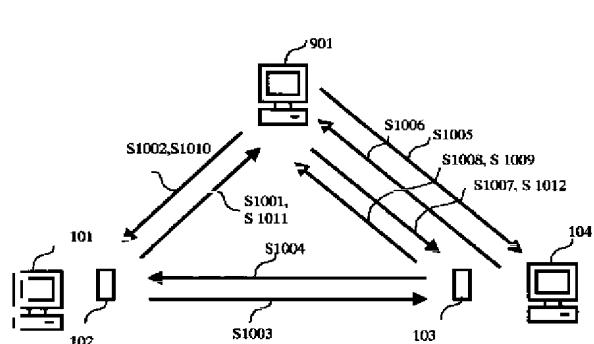
【図21】従来技術におけるネットワーク接続装置の構成の概略。

【符号の説明】

101、104、105、106	コンピュータ
102、103	ネットワーク接続装置
109	インターネット
110、111	ユーザ認証装置



【図1】



【図10】

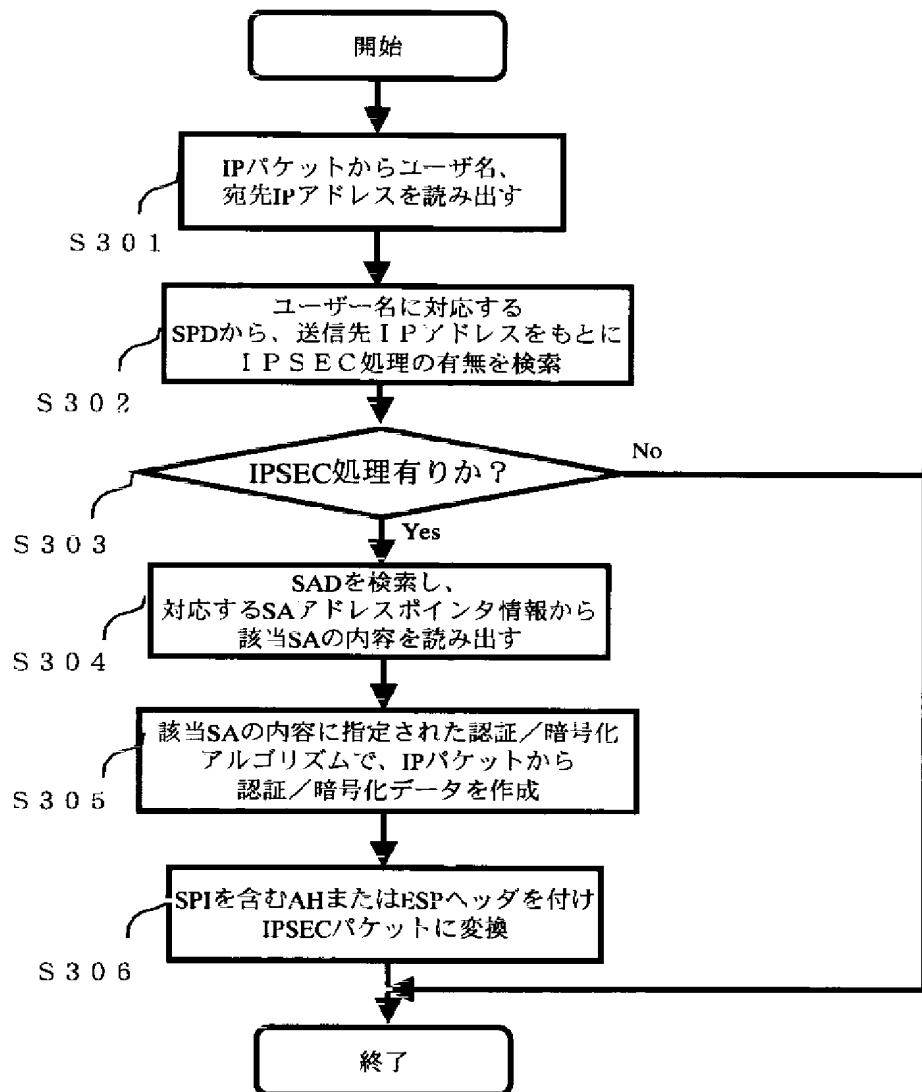
SPD-1		205	202	206	203	204
I PA-1 1	IP SEC - I PA-1 1	有		S A - 1 1		
I PA-1 2	IP SEC - I PA-1 2	無		—		
I PA-1 3	IP SEC - I PA-1 3	有		S A - 1 3		
-----	-----	-----		-----		
I PA-1 L	IP SEC - I PA-1 L	有		S A - 1 M		

SPD-N		201
I PA-1 1	IP SEC - I PA-N1	有
I PA-1 2	IP SEC - I PA-N2	無
I PA-1 3	IP SEC - I PA-N3	有
-----	-----	-----
I PA-N L	IP SEC - I PA-N L	有

【図2】

SAD-1		208	SAD-N	
209	アドレス情報	SAA-1	207	SA-N1
210	SPI	SPI-1		-----
211	認証アルゴリズム	HMAC-MD5		-----
212	暗号化アルゴリズム	DES-CBS	SAP	-----
213	-----	-----	-----	-----
214	-----	-----	-----	-----
215	-----	-----	-----	-----
216	-----	-----	-----	-----
217	-----	-----	-----	-----
218	-----	-----	-----	-----
219	-----	-----	-----	-----
220	-----	-----	-----	-----
221	-----	-----	-----	-----
222	-----	-----	-----	-----
223	-----	-----	-----	-----
224	-----	-----	-----	-----
225	-----	-----	-----	-----
226	-----	-----	-----	-----
227	-----	-----	-----	-----
228	-----	-----	-----	-----
229	-----	-----	-----	-----
230	-----	-----	-----	-----
231	-----	-----	-----	-----
232	-----	-----	-----	-----
233	-----	-----	-----	-----
234	-----	-----	-----	-----
235	-----	-----	-----	-----
236	-----	-----	-----	-----
237	-----	-----	-----	-----
238	-----	-----	-----	-----
239	-----	-----	-----	-----
240	-----	-----	-----	-----
241	-----	-----	-----	-----
242	-----	-----	-----	-----
243	-----	-----	-----	-----
244	-----	-----	-----	-----
245	-----	-----	-----	-----
246	-----	-----	-----	-----
247	-----	-----	-----	-----
248	-----	-----	-----	-----
249	-----	-----	-----	-----
250	-----	-----	-----	-----
251	-----	-----	-----	-----
252	-----	-----	-----	-----
253	-----	-----	-----	-----
254	-----	-----	-----	-----
255	-----	-----	-----	-----
256	-----	-----	-----	-----
257	-----	-----	-----	-----
258	-----	-----	-----	-----
259	-----	-----	-----	-----
260	-----	-----	-----	-----
261	-----	-----	-----	-----
262	-----	-----	-----	-----
263	-----	-----	-----	-----
264	-----	-----	-----	-----
265	-----	-----	-----	-----
266	-----	-----	-----	-----
267	-----	-----	-----	-----
268	-----	-----	-----	-----
269	-----	-----	-----	-----
270	-----	-----	-----	-----
271	-----	-----	-----	-----
272	-----	-----	-----	-----
273	-----	-----	-----	-----
274	-----	-----	-----	-----
275	-----	-----	-----	-----
276	-----	-----	-----	-----
277	-----	-----	-----	-----
278	-----	-----	-----	-----
279	-----	-----	-----	-----
280	-----	-----	-----	-----
281	-----	-----	-----	-----
282	-----	-----	-----	-----
283	-----	-----	-----	-----
284	-----	-----	-----	-----
285	-----	-----	-----	-----
286	-----	-----	-----	-----
287	-----	-----	-----	-----
288	-----	-----	-----	-----
289	-----	-----	-----	-----
290	-----	-----	-----	-----
291	-----	-----	-----	-----
292	-----	-----	-----	-----
293	-----	-----	-----	-----
294	-----	-----	-----	-----
295	-----	-----	-----	-----
296	-----	-----	-----	-----
297	-----	-----	-----	-----
298	-----	-----	-----	-----
299	-----	-----	-----	-----
300	-----	-----	-----	-----
301	-----	-----	-----	-----
302	-----	-----	-----	-----
303	-----	-----	-----	-----
304	-----	-----	-----	-----
305	-----	-----	-----	-----
306	-----	-----	-----	-----
307	-----	-----	-----	-----
308	-----	-----	-----	-----
309	-----	-----	-----	-----
310	-----	-----	-----	-----
311	-----	-----	-----	-----
312	-----	-----	-----	-----
313	-----	-----	-----	-----
314	-----	-----	-----	-----
315	-----	-----	-----	-----
316	-----	-----	-----	-----
317	-----	-----	-----	-----
318	-----	-----	-----	-----
319	-----	-----	-----	-----
320	-----	-----	-----	-----
321	-----	-----	-----	-----
322	-----	-----	-----	-----
323	-----	-----	-----	-----
324	-----	-----	-----	-----
325	-----	-----	-----	-----
326	-----	-----	-----	-----
327	-----	-----	-----	-----
328	-----	-----	-----	-----
329	-----	-----	-----	-----
330	-----	-----	-----	-----
331	-----	-----	-----	-----
332	-----	-----	-----	-----
333	-----	-----	-----	-----
334	-----	-----	-----	-----
335	-----	-----	-----	-----
336	-----	-----	-----	-----
337	-----	-----	-----	-----
338	-----	-----	-----	-----
339	-----	-----	-----	-----
340	-----	-----	-----	-----
341	-----	-----	-----	-----
342	-----	-----	-----	-----
343	-----	-----	-----	-----
344	-----	-----	-----	-----
345	-----	-----	-----	-----
346	-----	-----	-----	-----
347	-----	-----	-----	-----
348	-----	-----	-----	-----
349	-----	-----	-----	-----
350	-----	-----	-----	-----
351	-----	-----	-----	-----
352	-----	-----	-----	-----
353	-----	-----	-----	-----
354	-----	-----	-----	-----
355	-----	-----	-----	-----
356	-----	-----	-----	-----
357	-----	-----	-----	-----
358	-----	-----	-----	-----
359	-----	-----	-----	-----
360	-----	-----	-----	-----
361	-----	-----	-----	-----
362	-----	-----	-----	-----
363	-----	-----	-----	-----
364	-----	-----	-----	-----
365	-----	-----	-----	-----
366	-----	-----	-----	-----
367	-----	-----	-----	-----
368	-----	-----	-----	-----
369	-----	-----	-----	-----
370	-----	-----	-----	-----
371	-----	-----	-----	-----
372	-----	-----	-----	-----
373	-----	-----	-----	-----
374	-----	-----	-----	-----
375	-----	-----	-----	-----
376	-----	-----	-----	-----
377	-----	-----	-----	-----
378	-----	-----	-----	-----
379	-----	-----	-----	-----
380	-----	-----	-----	-----
381	-----	-----	-----	-----
382	-----	-----	-----	-----
383	-----	-----	-----	-----
384	-----	-----	-----	-----
385	-----	-----	-----	-----
386	-----	-----	-----	-----
387	-----	-----	-----	-----
388	-----	-----	-----	-----
389	-----	-----	-----	-----
390	-----	-----	-----	-----
391	-----	-----	-----	-----
392	-----	-----	-----	-----
393	-----	-----	-----	-----
394	-----	-----	-----	-----
395	-----	-----	-----	-----
396	-----	-----	-----	-----
397	-----	-----	-----	-----
398	-----	-----	-----	-----
399	-----	-----	-----	-----
400	-----	-----	-----	-----
401	-----	-----	-----	-----
402	-----	-----	-----	-----
403	-----	-----	-----	-----
404	-----	-----	-----	-----
405	-----	-----	-----	-----
406	-----	-----	-----	-----
407	-----	-----	-----	-----
408	-----	-----	-----	-----
409	-----	-----	-----	-----
410	-----	-----	-----	-----
411	-----	-----	-----	-----
412	-----	-----	-----	-----
413	-----	-----	-----	-----
414	-----	-----	-----	-----
415	-----	-----	-----	-----
416	-----	-----	-----	-----
417	-----	-----	-----	-----
418	-----	-----	-----	-----
419	-----	-----	-----	-----
420	-----	-----	-----	-----
421	-----	-----	-----	-----
422	-----	-----	-----	-----
423	-----	-----	-----	-----
424	-----	-----	-----	-----
425	-----	-----	-----	-----
426	-----	-----	-----	-----
427	-----	-----	-----	-----
428	-----	-----	-----	-----
429	-----	-----	-----	-----
43				

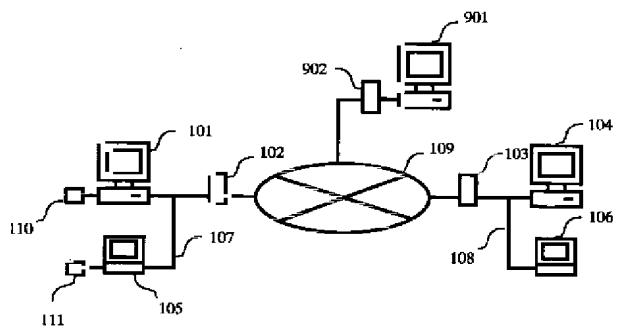
【図3】



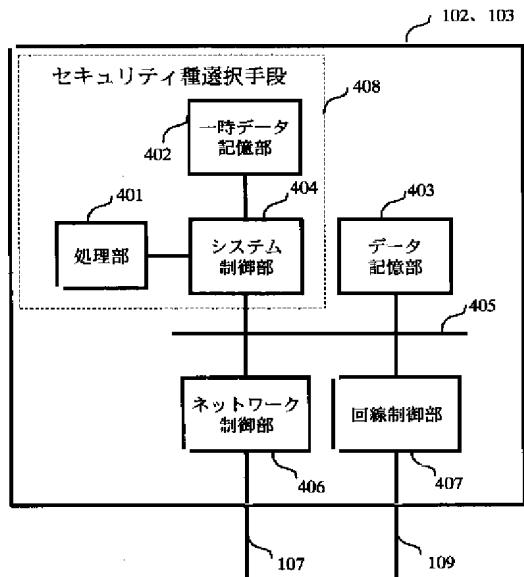
【図5】

501 APA - 1	502 IPA - 1	503 IPSEC - IPA - 1	504 有	505 SA - 1
APA - 2	IPA - 2	IPSEC - IPA - 2	無	—
-----	IPA - 3	IPSEC - IPA - 3	有	SA - 3
-----	-----	-----	-----	-----
APA - L	IPA - L	IPSEC - IPA - L	有	SA - M

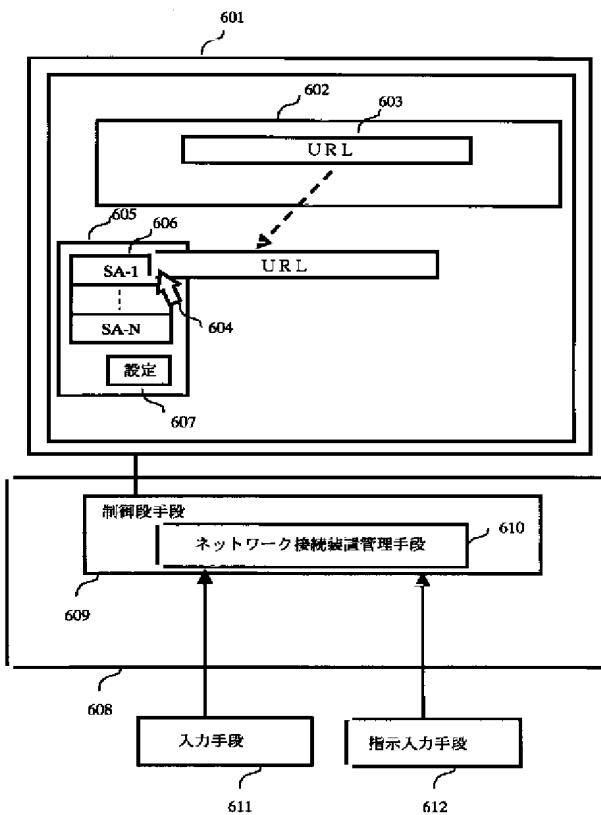
【図9】



【図4】



【図6】



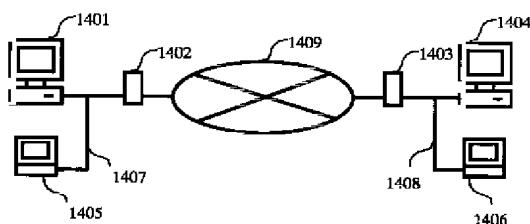
〔図8〕

SPD-1	501	202	206	203
APA-11	IPA-11	IPSEC-IPA-11	有	SA-11
APA-12	IPA-12	IPSEC-IPA-12	無	—
-----	IPA-13	IPSEC-IPA-13	有	SA-13
-----	-----	-----	-----	-----
APA-1L	IPA-1L	IPSEC-IPA-1L	有	SA-1M
SPD-N				801
APA-N1	IPA-N1	IPSEC-IPA-N1	有	SA-N1
APA-N2	IPA-N2	IPSEC-IPA-N2	無	—
-----	IPA-N3	IPSEC-IPA-N3	有	SA-N3
-----	-----	-----	---	-----
APA-NL	IPA-NL	IPSEC-IPA-NL	有	SA-NM

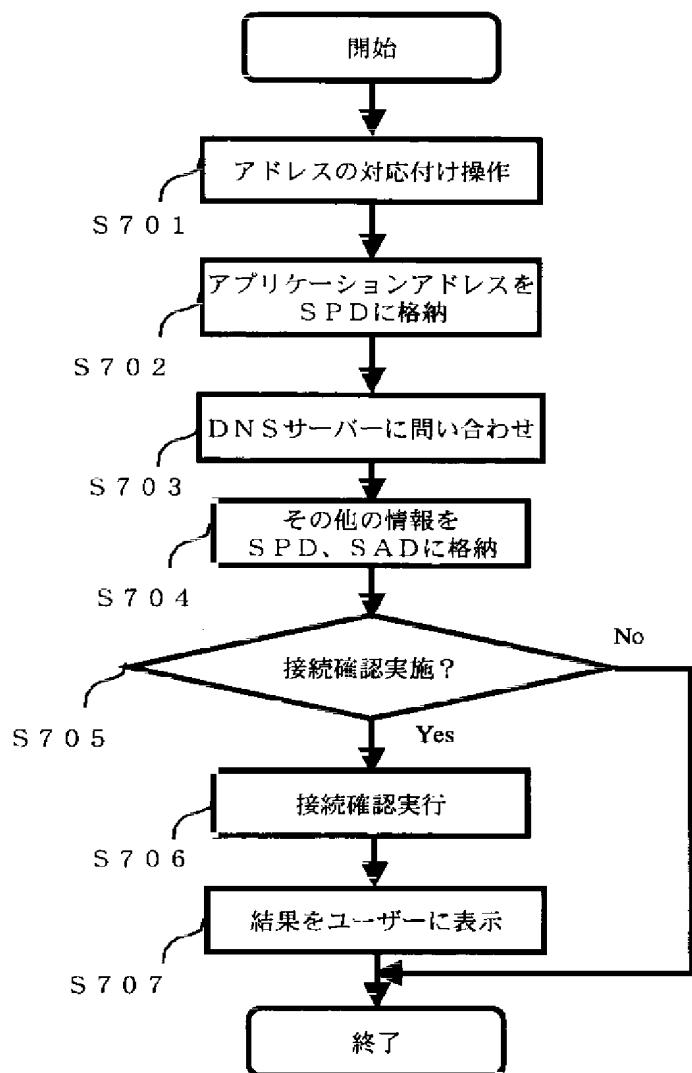
【习11】

I PA-1	I PSEC-I PA-1	有	SA-1
I PA-2	I PSEC-I PA-3	有	SA-2
-----	-----	-----	-----
I PA-L	I PSEC-I PA-L	無	-

〔図14〕



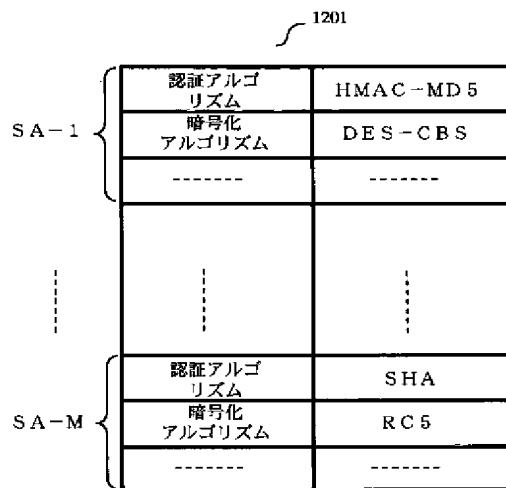
【図7】



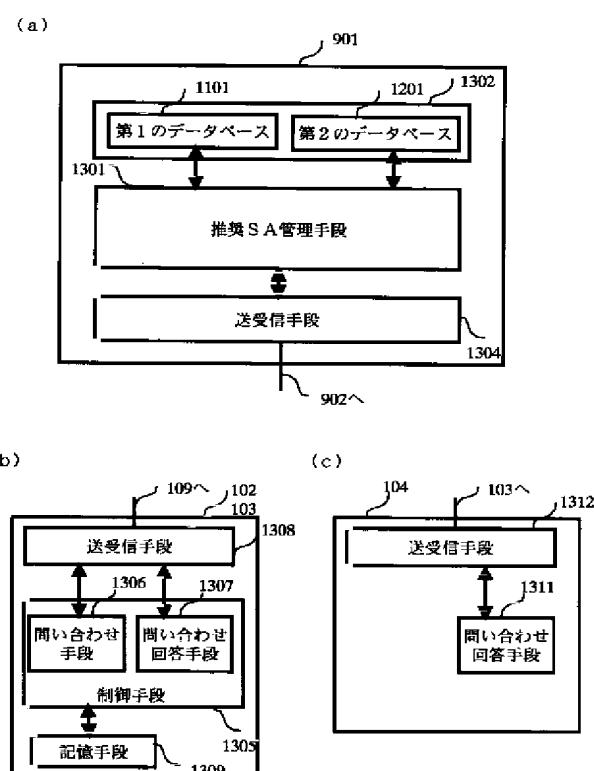
【図17】

IPA-1	IPSEC-IPA-1	有	SA-1
IPA-2	IPSEC-IPA-2	無	—
IPA-3	IPSEC-IPA-3	有	SA-3
-----	-----	-----	-----
IPA-L	IPSEC-IPA-L	有	SA-M

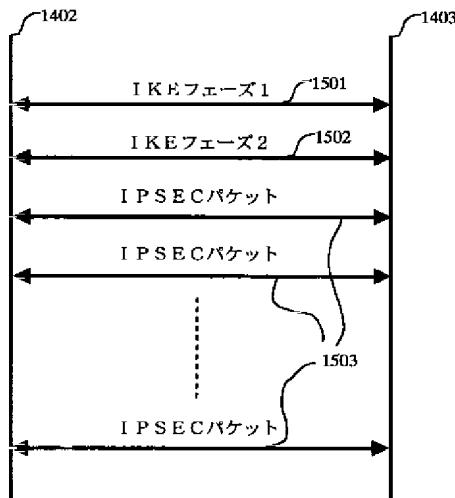
【図12】



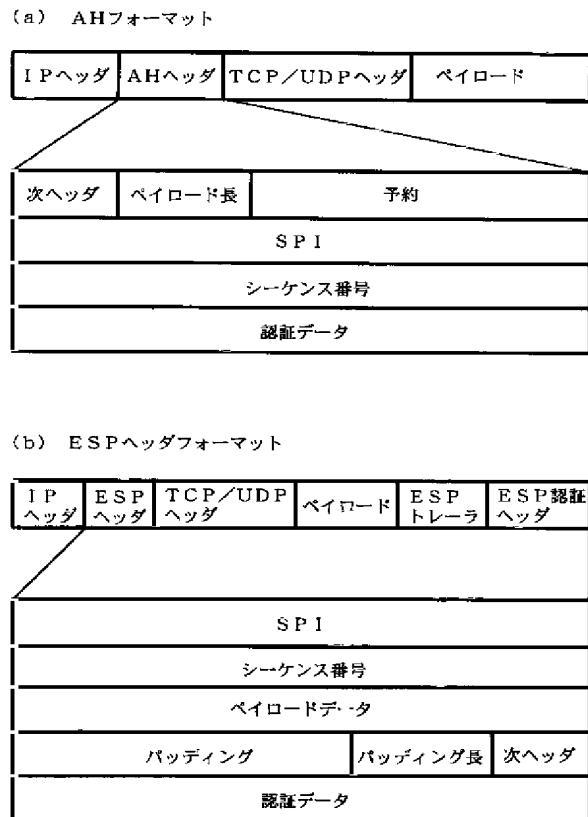
【図13】



【図15】



【図16】



【図18】

1801

アドレス情報	SAA-1
S P I	SPI -1
認証アルゴリズム	HMAC-MD5
暗号化アルゴリズム	DES-CBS
-----	-----
-----	-----
-----	-----

1802 SA-1 {

1804 } 1805

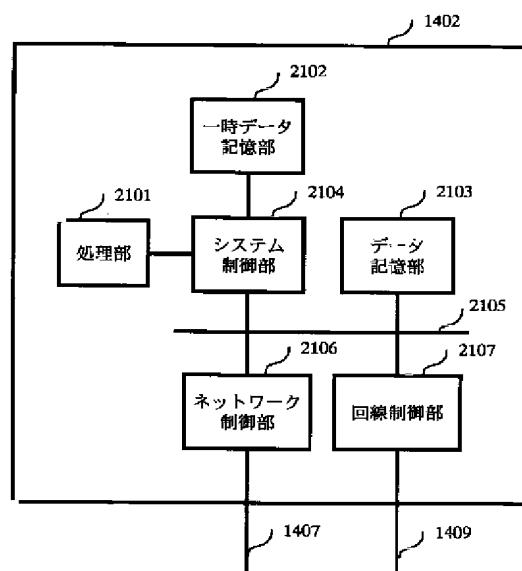
SAP-1

IPアドレス	SAA-M
S P I	SPI -M
認証アルゴリズム	SHA
暗号化アルゴリズム	Triple-DES
-----	-----

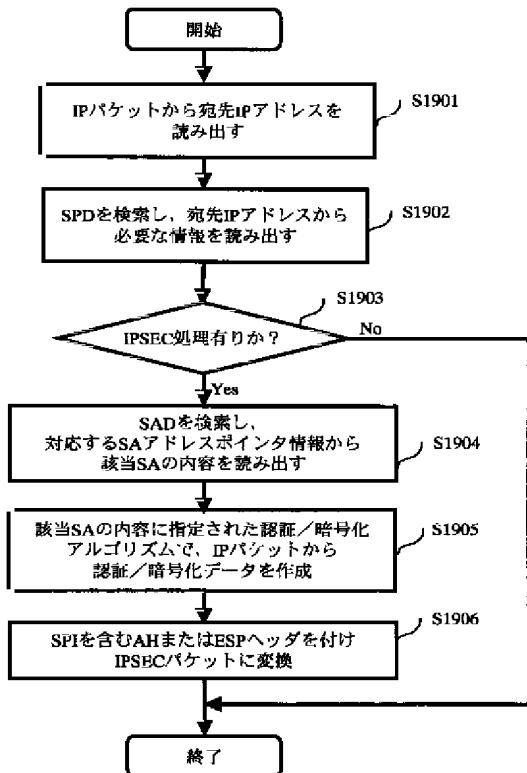
1803 SA-M {

1806 } SAP-M

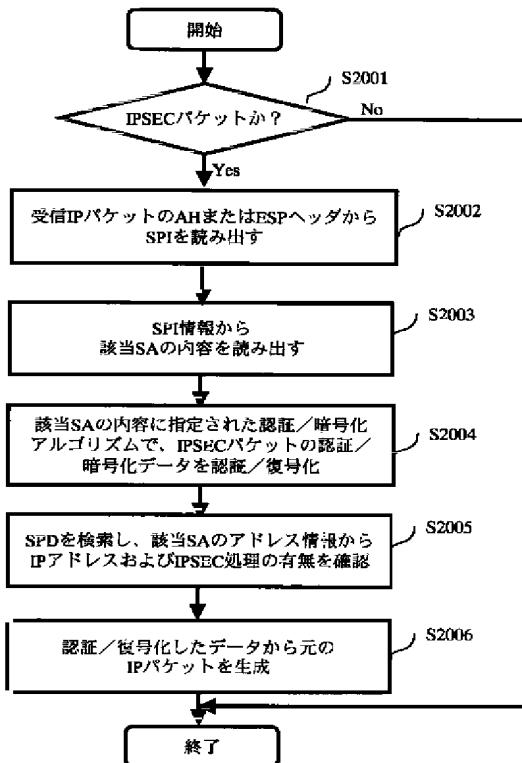
【図21】



【図19】



【図20】



フロントページの続き

(72)発明者 山内 弘貴
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 太田 雄策
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
F ターム(参考) 5B085 AE04 AE29
5J104 AA07 AA37 DA03 KA01 PA07